ЛЕКЦИЯ 14

ЗАЩИТА ИНФОРМАЦИИ В ИТ

Заключительная лекция будет посвящена вопросам защиты информации в ИТ системах.

1. Юридические основания

В этой части будет проведен обзор основных нормативно-законодательных актов, по которым предоставляются услуги и формируется базовое решение по защите информации.

Основными механизмами в части внедрения проектов по защите информации служит выполнение нормативов законодательства. К сожалению, понимание нужности тех или иных систем информационной безопасности приходит только лишь после инцидентов. Понятно, что инциденты наиболее заметны и наиболее значимы в крупных компаниях, поэтому внедрение систем защиты информации в российских компаниях началось где-то между 1994 и 1995 годами. Прежде всего внедрением занялись Центральный банк, Сбербанк, разные нефтяные компании, газовые компании. Все остальные компании занялись этим вопросом гораздо позже и уже исходя из обязательных нормативных требований.

В 1995 году начали внедрять информационную безопасность благодаря тому, что произошел целый ряд инцидентов с фальшивыми чеченскими авизо, которые вводились в платежную систему Центрального банка и Сбербанка, при этом они не были обеспечены никакими деньгами. С появлением этих авизо был издан первый закон о защите информации. Впоследствии, тоже в результате целой серии инцидентов, в систему защиты информации начали внедряться в крупных государственных компаниях. Надо понимать, что если вопрос защиты государственной тайны обязателен (он очень жестко регулируется государством), то вопросом защиты коммерческой тайны ранее занимались компании. Естественно, далеко не каждая компания была согласна отдавать деньги за то, что руководители компании не понимали до конца.

Впоследствии ситуация изменилась, и на текущий момент ключевым является перечень нормативных актов, которыми регулируется область защиты информации.

В равной степени при создании системы защиты информации важны следующие факторы:

1. **Документация**;

2. **Люди**;

3. **Оборудование и программное обеспечение**.

Как только при создании системы защиты информации возникает перекос в ту или иную сторону, сразу появляется разбалансировка, и в случае каких-либо специфических угроз не обнаружится должного образа защиты.

В качестве примера можно привести Федеральный закон № 152 «О защите персональных данных».

Возможно спроектировать собственную информационную систему так, что правильно составленная документация будет достаточным условием для того, чтобы у регуляторов не возникало вопросов относительного того, как сделана конкретная система защиты информации, но это не защитит компанию от атак хакера с достаточным опытом. Аналогично, может случиться обратная ситуация, когда после покупки оборудования и программного обеспечения, даже если его грамотно установить и настроить, руководство забывает обучить людей правилам эксплуатации этого оборудования и ПО. В какой-то момент можно получить ситуацию, когда будет заблокировано важное бизнес-приложение. И как результат, компания потеряет имидж, определенные деньги.

То же самое касается оборудования, ПО. В него тоже можно не вложиться до конца: все вложить в людей, оставив минимум документации и минимум оборудования, ПО. В принципе, так или иначе, это будет относительно эффективно, но никто не застрахован от проверки регуляторов. После проверки и обнаружения каких-либо несоответствий могут выписать довольно серьезное предписание, после чего руководитель будет отвечать за выполнение этих нормативных требований, причем не только финансово, но и вплоть до уголовной ответственности.

Приведем краткий перечень нормативной базы Российской Федерации, международной нормативной базы, которая актуальна для коммерческих (и не только) и для государственных компаний на текущий момент.

1. **Закон «О защите персональных данных»**.

   Этот закон наиболее распространен, поскольку персональные данные обрабатывает любая организация, которая присутствует на территории Российской Федерации. Таких организаций насчитывается порядка 800 тысяч.

   У любого человека есть все основания задавать вопрос о том, как к определенным организациям попали его персональные данные (такие как, сотовый телефон, фамилия, имя, отчество).

2. **Федеральный закон ФЗ-161 «О национальной платежной системе»**.

   Если у кого-либо украдут карту, и потерпевший выполнит своевременно все условия, которые предписал банк в договоре (а именно условие того, что потерпевший своевременно сообщит банку о краже), то в соответствии с этим законом сумму денег, которая будет снята с карты в этот период, банк должен возместить потерпевшему.

   В этом законе прописано много разных условий, которые накладываются на банки и платежные системы, платежные терминалы и все, что относится к Национальной платежной системе, которые должны выполнить компании, что весьма непросто.

Этот закон, несмотря на ряд недостатков, спас отрасль в 2008 году. Во время кризиса отрасль информационной безопасности просто прекратила свой рост благодаря лишь этому закону.

3. Ранее действовал **закон «О защите коммерческой тайны»**. В принципе, он отличается от действующего ныне закона рядом формулировок.

   В этом законе речь идет о конфиденциальных сведениях. Это актуально при приеме сотрудников на работу, требующую допуска к государственной тайне. Проверить корректность составления контракта можно прежде всего ознакомившись с законом.

4. **Закон «О защите государственной тайны»**.

5. Следующий нормативный акт — это **стандарт Банка России по обеспечению информационной безопасности (СТО ИББС)**. Он регулирует процесс обеспечения защиты информации в банках. Он также дублирует Закон «О защите персональных данных».

   Если банк выполняет требования СТО ИББС, которые не являются обязательными, но вполне могут ими стать, то Закон «О защите персональных данных» банк выполнять не обязан, поскольку требования защиты персональных данных включены в стандарт.

   Если Центральный банк все-таки сформирует свое подразделение контроля в части защиты информации (у него просто нет такого подразделения), то данный стандарт станет обязателен для всех банков.

6. **Стандарт PSI DSS**.

   Данный стандарт является стандартом компаний VISA и MasterCard, и он регулирует вопросы информационной безопасности в части платежных систем именно пластиковых карт.

7. **Международный стандарт ISO 2700X**.

   «X» обозначает, что выходят новые версии.

2. Общий подход к созданию информационной безопасности в ИТ

Первый этап создания информационной безопасности — это **обследование**. Обследования могут быть разные: как инструментальные, так и экспертные.

Под **инструментальными исследованиями** подразумевается, например, следующее: фиксируются все выходы информационной системы в Интернет, после чего проводится тестирование. Тестирование проводится соответствующими сканерами информационной безопасности, выявляются определенные уязвимости, и тестировщик выполняет роль хакера — он пытается их эксплуатировать, проникнуть в сеть, получить логины и пароли и взломать ее, получить важную информацию.

Экспертный аудит подразумевает анализ рисков. Анализируются прежде всего

документация, требования и знания, люди и в гораздо меньшей степени оборудование.

Существует также **аудит на соответствие нормативным требованиям**. Он тесно связан с Законом «О персональных данных» СТР К 527001, 59 DSS и ББС. Нужно проверить, что выполняется, что не выполняется, чего не хватает и в дальнейшем это устранить, чтобы сделать это до прихода соответствующей проверки. Очень часто те компании, которые просто откладывают приведение своей информационной сети в соответствии к законодательству на последний день, когда узнают, что у них будет проверка, сразу же начинают пытаться решить проблемы, но делают это слишком быстро. Многие интеграторы этим пользуются: они находят в открытых ресурсах график проверок и предварительно начинают уведомлять соответствующие предприятия.

Следующий этап довольно комплексный: по результатам обследования компании пишут **отчет**. Отчет включает в себя не просто перечисление проблем, но и методы их решения. Собственно, один из самых простых — это установка все обновлений сети и постоянный контроль этих обновлений. На самом деле, отчет включает большой перечень: на него уходит примерно месяц, поскольку информации туда попадает очень много.

На следующем этапе подготавливается **Концепция информационной безопасности**. Иногда её пропускают и начинают писать **модель угроз**. Рассматриются разные угрозы, в том числе и те, которые кажутся маловероятными (например, те, которые включают в себя нападение инопланетян).

Далее следует **модель нарушителя**, то есть описание того человека, которому будет интересна информационная система. В случае с персональными данными это Федеральная служба по техническому экспортному контролю. В некоторых случаях, если, опять же, это органы госвласти, кроме всего прочего утверждается также ФСБ. Утверждение новой составляющей — сложный процесс. Выдвигается много замечаний к нормативной документации, и написание всех документов занимает достаточное время. Разрабатывают два базовых документа: **техническое задание** и **технорабочий проект**. В них описывается план системы защиты информации. После этого разрабатывается вся остальная документация. В идеале, лучше в итоге получить Концепцию информационной безопасности чтобы понимать, как вообще будет развиваться информационная безопасность компании и как на этом можно сэкономить деньги (потому что каждый год внедрять новые решения довольно затратно). И в случае, если действовать рефлективным методом (то есть бороться с подобными проблемами по мере их поступления, а не работать над причиной их возникновения), не исключено, что проблемы будут требовать каких-то кардинальных решений и поворотов во взгляде на информационную безопасность.

Следующий этап — это **создание комплексной системы управления информационной безопасностью**.

Помимо организационной части существует еще и **техническая часть**, которая привязана к системе управления информационной безопасностью. Например, анализ защищенности в части уязвимости без соответствующего сканера уязвимости сделать невозможно. Мониторинг событий информационной безопасности тоже требует технических средств. Также потребуется система предотвращения вторжений, система сбора и анализа журналов событий со всех остальных средств защиты информации (антивирус, сетевой экран, система разграничения доступа).

Необходимо будет решать две задачи: информационной безопасности и обеспечения

непрерывности бизнеса. В принципе, это две разные задачи, но решать их совместно — наиболее выгодный путь.

Управление изменениями, управление учетными записями — тоже обязательные части защиты информации.

3. Аудит информационной безопасности

Цель аудита информационной безопасности — получение объективной оценки состояния информационной безопасности в компании.

Во многих государственных компаниях (и особенно органах госвласти), где персонал не меняется годами, обычно не проводится никакое специализированное обучение. Если там проводить аудит, то с большой вероятностью окажется, что пароли никто не менял в течение долгого времени, причем вместо одного человека их знает весь отдел.

Можно также узнать, насколько защищена вся система в целом. Часто новое оборудование забывают внедрять (но по документам оно присутствует).

Иногда случается обратная ситуация: продавцы, исходя из собственных интересов, убеждают руководство, что компании любого органа госвласти просто необходимо купить соответствующее оборудование либо программное обеспечение. При этом никто не обращает внимание, насколько эффективно будет работать данное ПО в существующей сети.

Чтобы понимать, насколько часто происходят инциденты информационной безопасности, приведём статистику с проекта по внедрению системы «Сбор и анализ журналов событий» в одной негосударственной организации. Буквально за сутки зафиксировали 77 тысяч инцидентов. 50 тысяч из них — трафик из Китая.

4. Концепция информационной безопасности

В результате общего взгляда на безопасность и глядя на прогнозы развития ландшафта угроз и развития средств защиты информации, вырабатывается несколько дополнительных документов более приземленного уровня. Это **корпоративная политика информационной безопасности** (прежде всего), **частные политики информационной безопасности**, и уже непосредственно **требования к процедурам** (детали обеспечения процедуры антивирусной защиты информации в компании).

В качестве примера более общей концепции безопасности можно привести концепцию безопасности города Москвы. Главная проблема Москвы на текущий момент — это отсутствие достаточного количества качественной воды (не только питьевой, но и технической). Предприятия потребляют её в достаточных количествах. Фильтровать воду сложно — нужны очень большие фильтры. Это будет очень дорого. Либо, если использовать природную фильтрацию, нужен дополнительный объем воды, потому что вода должна пройти цикл: «естественная фильтрация в почве – выход из почвы – испарения – дожди». Поскольку на него просто не хватает времени (воду выпивают раньше, чем она проходит этот цикл), то и качество воды резко падает.

В местах, где площадь города намного меньше площади Москвы, а населения больше, есть другие пути решения. Там совершенно другой климат. Также обычно опресняют морскую воду с параллельным использованием ее в качестве технической воды.

5. Стандарты

Часть стандартов доступна к ознакомлению, поэтому в этом разделе информация о них будет представлена кратко.

5.1. ISO27001

Надо отметить, что кроме серии 27 есть довольно большое количество стандартов ISO в части информационной безопасности. Рассматриваемый стандарт является одним из первых, поэтому на него многие ранее ориентировались. Сейчас его крайне редко используют для внедрения, но раньше он был востребован в основном филиалами западных компаний в России.

Он регламентирует вопросы управления информационной безопасности и создания системы управления информационной безопасности.

Под сертификацией, которой подвергается система управления, подразумевается не сертификация ФСТЭКа и ФСБ, а сертификация в компаниях, которые являются сами сертифицированными аудиторами по данному стандарту (то есть, те компании, у которых есть достаточное количество обученного персонала и опыта изучения и внедрения подобных систем).

5.2. Режим коммерческой тайны

Любая информация, представляющая ценность для компании, является коммерческой тайной.

Политика обеспечения коммерческой тайны — это установление режима коммерческой тайны на предприятии (то есть, не только соглашение с сотрудниками, но и описание всего, что входит в него — например, сведений, которые отнесены к коммерческой тайне).

5.3. Защита персональных даных

К персональным данным относятся те данные, которые содержат нечто большее, чем фамилия, имя, отчество людей. Самый высокий класс персональных данных — это медицина и религия (это первый класс персональных данных, которые должны защищаться наиболее серьезно).

Пока человек не подпишет соглашение о предоставлении его персональных данных для обработки, его личные данные компания не будет иметь права обрабатывать.

5.4. СТО ИББС

СТО ИББС — это серия отраслевых стандартов, которые регламентируют организационную часть в ряде нормативных документов, которые должны быть в банке, и техническую часть. С помощью этих стандартов регламентируют те решения, которые тоже должны применяться для защиты банковских систем.

5.5. PCI DSS

В этом стандарте прописаны требования, которым должны соответствовать платежные системы VISA и MasterCard.

Он включает обязательные ревизии, обязательный аудит тех систем, которые применяются. В нем прописана финансовая ответственность аудитора за инциденты (аудитор несет ответственность до 1 млн евро для возмещения ущерба банкам). Соответственно, эта система находится под страховкой.

5.6. Создание процессов управления информационной безопасностью

Это достаточно непростая процедура. Здесь важны основные принципы: система управления информационной безопасностью должна охватывать все значимые информационные системы. Если упустить ряд деталей, стойкость системы всегда будет оцениваться по слабому звену.

5.7. Подсистема информационной безопасности

Это технические меры для системы управления информационной безопасностью (то есть, те решения, которые будут собирать данные, обрабатывать данные и передавать в общую систему мониторинга).

На инциденты необходимо реагировать. В штате необходим сотрудник, который будет заниматься мониторингом всего, что происходит в сети. Без такого сотрудника система проработает какое-то время, но после первого серьезного инцидента работа завершится.